EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S3	0	713/190-192	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 14:57
S4	605	(713/190-192).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/25 17:01
S5	416	(713/190-192).CCLS.	USPAT	OR	OFF	2007/07/23 15:55
S6	17	cryptographic adj provider	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 15:55
S7	1	(encrypt$3 scrambl$3 cryptographic) same (asynchronous with synchronous with request)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 16:06
S8	321	(encrypt$3 scrambl$3 cryptographic) and (asynchronous with synchronous with request)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 16:07
S9	14	(encrypt$3 scrambl$3 cryptographic). ab. and (asynchronous with synchronous with request)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 16:20
S10	191	cryptographic adj accelerator	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 16:26
S12	394	(cryptographic encrypt$3) near3 accelerator	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 16:27

EAST Search History

S15	29	(cryptographic encrypt$3) near3 accelerator and (asynchronous and synchronous)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 16:41
S16	13	(cryptographic encrypt$3) near3 accelerator and (asynchronous same synchronous)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 16:42
S17	2	("6910133").URPN.	USPAT	OR	ON	2007/07/23 16:50
S18	21	("4161719" | "4672534" | "5241599" | "5291482" | "5303237" | "5345446" | "5351136" | "5361362" | "5416842" | "5561669" | "5734654" | "5764772" | "5793763" | "5913045" | "5920572" | "5941964" | "5953336" | "6064677" | "6067301" | "6320964" | "6519636"). PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/23 16:52
S19	156	schedul$3 same (cryptographic encrypt$3 scrambl$3) same (hardware same software)	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/23 16:54
S20	24	schedul$3 same (cryptographic encrypt$3 scrambl$3) same (synchronous same asynchronous)	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/23 16:56
S22	119	(713/192).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/23 18:18
S23	119	(713/192).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/23 18:18
S24	16	S23 and (asynchronous)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 18:22
S25	3	(encrypt$3 cryptograph$2) same (kernel) same (asynchronous same synchronous)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 18:24
S26	1	("4,961,221").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/23 18:25

EAST Search History

S27	8	(cryptographic adj framework).ab.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 18:27
S28	339	(select$3 chos$3) with (encrypt$3 cryptographic) same (hardware same software)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 18:29
S29	18	("20020083318" | "5048086" | "5201000" | "5343527" | "5612682" | "5651067" | "5706489" | "5778072" | "5835600" | "5901227" | "6028939" | "6070198" | "6122742" | "6393565" | "6523119" | "6671809" | "6672505" | "6963980").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/23 18:44
S30	0	("7120799").URPN.	USPAT	OR	ON	2007/07/23 20:48
S31	1	("20040255145").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/23 20:50
S32	1134	schedul$3 with (cryptographic encrypt$3 scrambl$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 20:51
S33	152	schedul$3 with (cryptographic encrypt$3 scrambl$3) not operation	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 21:01
S34	0	(synchronous same asynchronous) same (hardware adj mode same software adj mode)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 21:02
S35	0	(synchronous same asynchronous) same (hardware adj provider same software adj provider)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 21:02

EAST Search History

S36	568	(synchronous same asynchronous) same (hardware same software)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 21:02
S37	29	(synchronous same asynchronous) same (hardware same software) same (cryptographic encrypt$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 21:05
S38	17	(synchronous same asynchronous) same (hardware same software) same (kernel)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 21:05
S39	18	("20020083318" | "5048086" | "5201000" | "5343527" | "5612682" | "5651067" | "5706489" | "5778072" | "5835600" | "5901227" | "6028939" | "6070198" | "6122742" | "6393565" | "6523119" | "6671809" | "6672505" | "6963980").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/23 21:08
S40	1	("6028939").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/24 17:29
S41	1	("5778072").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/24 17:30
S47	4485	asynchronous same queue	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 18:20
S48	2258	asynchronous with queue	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 18:20
S49	559	synchronous same asynchronous with queue	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 18:20
S50	269	synchronous same asynchronous with queue	USPAT	OR	ON	2007/07/25 18:56

EAST Search History

S51	37	synchronous same asynchronous with queue same interrupt	USPAT	OR	ON	2007/07/26 01:42
S53	573	determin$3 with synchronous with asynchronous	USPAT	OR	ON	2007/07/25 19:42
S54	196	determin$3 near4 synchronous with asynchronous	USPAT	OR	ON	2007/07/25 19:42
S55	149	determin$3 near4 synchronous near4 asynchronous	USPAT	OR	ON	2007/07/25 19:54
S56	4	determin$3 near4 synchronous near4 asynchronous same queue	USPAT	OR	ON	2007/07/25 20:05
S57	25	determin$3 with synchronous with asynchronous same queue	USPAT	OR	ON	2007/07/25 20:05
S58	75	determin$3 with synchronous with asynchronous same queue	US-PGPUB; USPAT	OR	ON	2007/07/25 21:04
S59	10	determin$3 near4 synchronous near4 asynchronous same queue	US-PGPUB; USPAT	OR	ON	2007/07/25 20:05
S60	11	determin$3 with synchronous with asynchronous same queue same available	US-PGPUB; USPAT	OR	ON	2007/07/25 20:15
S61	0	determin$3 with synchronous with asynchronous same "not" near3 queue	US-PGPUB; USPAT	OR	ON	2007/07/25 21:05
S62	0	asynchronous same "not" near3 queue	US-PGPUB; USPAT	OR	ON	2007/07/25 21:05
S63	0	"not" near3 "need" near4 queu$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 21:34
S64	152	synchronous near3 queue same asynchronous	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 22:51
S65	53	asynchronous with (indicat$3 specif$3 designat$3 tag$4) near3 queue	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:05
S66	291	asynchronous with (request) near3 queue	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:05

EAST Search History

S67	87	asynchronous with (request) near3 queued	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:11
S68	0	asynchronous with (request) near3 "to be queued"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:05
S70	362	notify with resource with available	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:17
S71	4	notify with resource with available same asynchronous	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:16
S72	100	notify with queue near3 available	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:18
S73	64	notify with (queue near2 available)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:27
S74	17345	(loading near4 (cryptographic encryption program))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:28
S75	7	(loading near4 ((cryptographic encryption) adj program))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:28

EAST Search History

S76	18	(loading near4 ((cryptographic encryption) adj (software algorithm program)))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:31
S77	1	(adding with (removing loading) with ((cryptographic encryption) adj (software algorithm program)))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:31
S78	1	(installing with (removing loading) with ((cryptographic encryption) adj (software algorithm program)))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:32
S79	18	(install$3 load$3 add$3) with (remov$3 delet$3) with ((cryptographic encryption) adj (software algorithm program))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 23:33
S80	62	synchronous same asynchronous same kernel	USPAT	OR	ON	2007/12/19 00:12
S82	29	synchronous same asynchronous same kernel same request	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/27 13:52
S83	1	("7013465").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/27 16:39
S84	1	("6546425").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/27 16:39
S85	667	(713/190-192).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/12/18 23:49
S86	57	S85 and (@pd > "20070727")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/18 23:49
S87	136	synchronous same asynchronous same kernel	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 00:12

EAST Search History

S88	20	synchronous same asynchronous same kernel and encrypt$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 00:13
S89	3	synchronous same asynchronous same kernel same encrypt$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 00:16
S90	3	synchronous same asynchronous same kernel same (cryptograph$3 encrypt$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 00:17
S91	1	(synchronous and asynchronous and kernel and (cryptograph$3 encrypt$3)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 01:13
S92	480	(713/164).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/12/19 01:13
S93	10	S92 and (asynchronous and synchronous)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 01:13
S94	5	("5043878" | "5774652" | "5948064" | "6131165" | "6154818").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/12/19 01:27

Terms used: **synchronous asynchronous kernel encryption** Found **96** of **216,199**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 96 Result page: **1** 2 3 4 5 next

Relevance scale

1 Evaluating network processing efficiency with processor partitioning and asynchronous I/O

Tim Brecht, G. (John) Janakiraman, Brian Lynn, Vikram Saletore, Yoshio Turner
April 2006 **ACM SIGOPS Operating Systems Review , Proceedings of the ACM SIGOPS/EuroSys European Conference on Computer Systems 2006 EuroSys '06**, Volume 40 Issue 4
Publisher: ACM
Full text available: pdf(521.28 KB) Additional Information: full citation, abstract, references, index terms

Applications requiring high-speed TCP/IP processing can easily saturate a modern server. We and others have previously suggested alleviating this problem in multiprocessor environments by dedicating a subset of the processors to perform network packet processing. The remaining processors perform only application computation, thus eliminating contention between these functions for processor resources. Applications interact with packet processing engines (PPEs) using an asynchronous I/O (AIO) prog ...

Keywords: TCP/IP, asynchronous I/O, network processing

2 Cryptography as an operating system service: A case study

Angelos D. Keromytis, Jason L. Wright, Theo De Raadt, Matthew Burnside
February 2006 **ACM Transactions on Computer Systems (TOCS)**, Volume 24 Issue 1
Publisher: ACM Press
Full text available: pdf(669.12 KB) Additional Information: full citation, abstract, references, index terms

Cryptographic transformations are a fundamental building block in many security applications and protocols. To improve performance, several vendors market hardware accelerator cards. However, until now no operating system provided a mechanism that allowed both uniform and efficient use of this new type of resource.We present the OpenBSD Cryptographic Framework (OCF), a service virtualization layer implemented inside the operating system kernel, that provides uniform access to accelerator functio ...

Keywords: Encryption, authentication, cryptographic protocols, digital signatures, hash functions

3 MANTIS OS: an embedded multithreaded operating system for wireless micro sensor platforms

Shah Bhatti, James Carlson, Hui Dai, Jing Deng, Jeff Rose, Anmol Sheth, Brian Shucker, Charles Gruenwald, Adam Torgerson, Richard Han
August 2005 **Mobile Networks and Applications**, Volume 10 Issue 4
Publisher: Kluwer Academic Publishers
Full text available: pdf(1.27 MB) Additional Information: full citation, abstract, references, index terms

The MANTIS MultimodAl system for NeTworks of In-situ wireless Sensors provides a new multithreaded cross-platform embedded operating system for wireless sensor networks. As sensor networks accommodate increasingly complex tasks such as compression/aggregation and signal processing, preemptive multithreading in the MANTIS sensor OS (MOS) enables micro sensor nodes to natively interleave complex tasks with time-sensitive tasks, thereby mitigating the bounded buffer producer-consumer problem. To ac ...

Keywords: cross-platform, dynamic reprogramming, embedded operating system, lightweight, low power, multithreaded, sensor networks

4 Securing ATM networks
Shaw-Cheng Chuang
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security CCS '96**
Publisher: ACM Press
Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

5 Profile-directed optimization of event-based programs
Mohan Rajagopalan, Saumya K. Debray, Matti A. Hiltunen, Richard D. Schlichting
May 2002 **ACM SIGPLAN Notices , Proceedings of the ACM SIGPLAN 2002 Conference on Programming language design and implementation PLDI '02**, Volume 37 Issue 5
Publisher: ACM Press
Full text available: pdf(167.69 KB) Additional Information: full citation, abstract, references, citings, index terms

Events are used as a fundamental abstraction in programs ranging from graphical user interfaces (GUIs) to systems for building customized network protocols. While providing a flexible structuring and execution paradigm, events have the potentially serious drawback of extra execution overhead due to the indirection between modules that raise events and those that handle them. This paper describes an approach to addressing this issue using static optimization techniques. This approach, which explo ...

Keywords: events, handlers, profiling

6 Distributed systems - programming and management: On remote procedure call
Patrícia Gomes Soares
November 1992 **Proceedings of the 1992 conference of the Centre for Advanced Studies on Collaborative research - Volume 2 CASCON '92**
Publisher: IBM Press
Full text available: pdf(4.52 MB) Additional Information: full citation, abstract, references, citings

The Remote Procedure Call (RPC) paradigm is reviewed. The concept is described, along with the backbone structure of the mechanisms that support it. An overview of works in supporting these mechanisms is discussed. Extensions to the paradigm that have been proposed to enlarge its suitability, are studied. The main contributions of this paper are a standard view and classification of RPC mechanisms according to different perspectives,

and a snapshot of the paradigm in use today and of goals for t ...

7 Storage: Generalized file system dependencies

Christopher Frost, Mike Mammarella, Eddie Kohler, Andrew de los Reyes, Shant Hovsepian, Andrew Matsuoka, Lei Zhang

October 2007 **Proceedings of twenty-first ACM SIGOPS symposium on Operating systems principles SOSP '07**

Publisher: ACM Press

Full text available: pdf(361.95 KB) Additional Information: full citation, abstract, references, index terms

Reliable storage systems depend in part on "write-before" relationships where some changes to stable storage are delayed until other changes commit. A journaled file system, for example, must commit a journal transaction before applying that transaction's changes, and soft updates and other consistency enforcement mechanisms have similar constraints, implemented in each case in system-dependent ways. We present a general abstraction, the patch, that makes write-before relationships explicit a ...

Keywords: dependencies, file systems, journaling, soft updates

8 Extending ACID semantics to the file system

Charles P. Wright, Richard Spillane, Gopalan Sivathanu, Erez Zadok

June 2007 **ACM Transactions on Storage (TOS)**, Volume 3 Issue 2

Publisher: ACM Press

Full text available: pdf(783.03 KB) Additional Information: full citation, abstract, references, index terms

An organization's data is often its most valuable asset, but today's file systems provide few facilities to ensure its safety. Databases, on the other hand, have long provided transactions. Transactions are useful because they provide atomicity, consistency, isolation, and durability (ACID). Many applications could make use of these semantics, but databases have a wide variety of nonstandard interfaces. For example, applications like mail servers currently perform elaborate error handling to ...

Keywords: File system transactions, databases, file systems, ptrace monitors, recoverable memory

9 Two years of experience with a &mgr;-Kernel based OS

Jochen Liedtke, Ulrich Bartling, Uwe Beyer, Dietmar Heinrichs, Rudolf Ruland, Gyula Szalay

April 1991 **ACM SIGOPS Operating Systems Review**, Volume 25 Issue 2

Publisher: ACM Press

Full text available: pdf(829.22 KB) Additional Information: full citation, abstract, citings, index terms

This paper describes the basic components of the L3 operating system and the experiences of the first two years using it. The system results from scientific research, but is addressed to commercial application. It is based on a small kernel handling tasks, threads and dataspaces. User level device drivers and file systems are described as examples of flexible OS services realized outside the kernel.

10 Aspect reuse and domain-specific approaches: Reflections on aspects and configurable protocols

Matti Hiltunen, François Taïani, Richard Schlichting

March 2006 **Proceedings of the 5th international conference on Aspect-oriented software development AOSD '06**

Publisher: ACM Press

Full text available: pdf(378.69 KB) Additional Information: full citation, abstract, references, index terms

The goals of aspect oriented software development (AOSD) and frameworks for configurable protocols (CPs) are similar in many respects. AOSD allows the specification of cross-cutting concerns called aspects as separate modules that are woven with the base program as needed. CPs are oriented towards building protocols or services with different quality of service (QoS) properties and attributes out of collections of independent modules, with each configuration customizing the service for a given a ...

Keywords: configurable software, extensible software

11 On randomization in sequential and distributed algorithms

Rajiv Gupta, Scott A. Smolka, Shaji Bhaskar
March 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 1
Publisher: ACM Press

Full text available: pdf(8.01 MB) Additional Information: full citation, abstract, references, citings, index terms

Probabilistic, or randomized, algorithms are fast becoming as commonplace as conventional deterministic algorithms. This survey presents five techniques that have been widely used in the design of randomized algorithms. These techniques are illustrated using 12 randomized algorithms—both sequential and distributed— that span a wide range of applications, including:primality testing (a classical problem in number theory), interactive probabilistic proof s ...

Keywords: Byzantine agreement, CSP, analysis of algorithms, computational complexity, dining philosophers problem, distributed algorithms, graph isomorphism, hashing, interactive probabilistic proof systems, leader election, message routing, nearest-neighbors problem, perfect hashing, primality testing, probabilistic techniques, randomized or probabilistic algorithms, randomized quicksort, sequential algorithms, transitive tournaments, universal hashing

12 Operating system structure: Making information flow explicit in HiStar

Nickolai Zeldovich, Silas Boyd-Wickizer, Eddie Kohler, David Mazières
November 2006 **Proceedings of the 7th symposium on Operating systems design and implementation OSDI '06**
Publisher: USENIX Association
Full text available: pdf(293.85 KB) Additional Information: full citation, abstract, references

HiStar is a new operating system designed to minimize the amount of code that must be trusted. HiStar provides strict information flow control, which allows users to specify precise data security policies without unduly limiting the structure of applications. HiStar's security features make it possible to implement a Unix-like environment with acceptable performance almost entirely in an untrusted user-level library. The system has no notion of superuser and no fully trusted code other than t ...

13 Horus: a flexible group communication system

Robbert van Renesse, Kenneth P. Birman, Silvano Maffeis
April 1996 **Communications of the ACM**, Volume 39 Issue 4
Publisher: ACM Press
Full text available: pdf(312.96 KB) Additional Information: full citation, references, citings, index terms

14 SCONE: using concurrent objects for low-level operating system programming

Jun-ichiro Itoh, Yasuhiko Yokote, Mario Tokoro

October 1995 **ACM SIGPLAN Notices , Proceedings of the tenth annual conference on Object-oriented programming systems, languages, and applications OOPSLA '95**, Volume 30 Issue 10

Publisher: ACM Press

Full text available: pdf(1.66 MB) Additional Information: full citation, abstract, references, citings, index terms

This paper proposes a methodology for making low-level system code of operating systems be replaceable at runtime. Our approach is to use concurrent objects as a basic programming unit for low-level system programs. To realize the different need for each type of system code and to execute these concurrent objects sufficiently efficient, we use a combination of dedicated system service layers and other implementation techniques. System service layers provide the most suitable primitive operations ...

15 Applications of DRM: Drm to counter side-channel attacks?

Ryad Benadjila, Olivier Billet, Stanislas Francfort

October 2007 **Proceedings of the 2007 ACM workshop on Digital Rights Management DRM '07**

Publisher: ACM

Full text available: pdf(238.48 KB) Additional Information: full citation, abstract, references, index terms

In the DRM setting, the attacker is a very powerful adversary, owning the software as well as the underlying hardware. This context is far different from the black-box attacker commonly considered in conventional cryptography.Therefore, cryptographers have tried to design new cryptographic tools fitting the DRM requirements. A related issuein cryptography is that of side-channel attacks, where theattacker is stronger than the black-box attacker, but usually weaker than a DRM attacker. In this ...

Keywords: AES, DRM, side-channel attacks, white-box

16 Secure deletion: Secure deletion myths, issues, and solutions

Nikolai Joukov, Harry Papaxenopoulos, Erez Zadok

October 2006 **Proceedings of the second ACM workshop on Storage security and survivability StorageSS '06**

Publisher: ACM Press

Full text available: pdf(135.60 KB) Additional Information: full citation, abstract, references, index terms

This paper has three goals. (1) We try to debunk several held misconceptions about secure deletion: that encryption is an ideal solution for everybody, that existing data-overwriting tools work well, and that securely deleted files must be overwritten many times. (2) We discuss new and important issues that are often neglected: secure deletion consistency in case of power failures, handling versioning and journalling file systems, and metadata overwriting. (3) We present two solutions for on-dem ...

Keywords: file systems, secure deletion, security, unintended data recovery

17 Emerging threats: A preliminary investigation of worm infections in a bluetooth environment

Jing Su, Kelvin K. W. Chan, Andrew G. Miklas, Kenneth Po, Ali Akhavan, Stefan Saroiu, Eyal de Lara, Ashvin Goel

November 2006 **Proceedings of the 4th ACM workshop on Recurring malcode WORM '06**

Publisher: ACM Press

Full text available: pdf(876.85 KB) Additional Information: full citation, abstract, references, index terms

Over the past year, there have been several reports of malicious code exploiting

vulnerabilities in the Bluetooth protocol. While the research community has started to investigate a diverse set of Bluetooth security issues, little is known about the feasibility and the propagation dynamics of a worm in a Bluetooth environment. This paper is an initial attempt to remedy this situation.We start by showing that the Bluetooth protocol design and implementation is large and complex. We gather traces ...

Keywords: Bluetooth, malware, worms

18 Exokernel: an operating system architecture for application-level resource management

D. R. Engler, M. F. Kaashoek, J. O'Toole

December 1995 **ACM SIGOPS Operating Systems Review , Proceedings of the fifteenth ACM symposium on Operating systems principles SOSP '95**, Volume 29 Issue 5

Publisher: ACM Press

Full text available: pdf(2.16 MB) Additional Information: full citation, references, citings, index terms

19 Separating key management from file system security

David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel

December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5

Publisher: ACM Press

Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index terms

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use.We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

20 Accent: A communication oriented network operating system kernel

Richard F. Rashid, George G. Robertson

December 1981 **ACM SIGOPS Operating Systems Review , Proceedings of the eighth ACM symposium on Operating systems principles SOSP '81**, Volume 15 Issue 5

Publisher: ACM Press

Full text available: pdf(1.01 MB) Additional Information: full citation, abstract, references, citings, index terms

Accent is a communication oriented operating system kernel being built at Carnegie-Mellon University to support the distributed personal computing project, Spice, and the development of a fault-tolerant distributed sensor network (DSN). Accent is built around a single, powerful abstraction of communication between processes, with all kernel functions, such as device access and virtual memory management accessible through messages and distributable throughout a network. In this paper, specif ...

Keywords: Distributed computation, Inter-process communication, Network, Networking, Operating systems, PERQ, Paging, UNIX, VAX, Virtual memory